UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/059,217	01/31/2002	Mikio Hashimoto	218943US2RD	6024

22850 7590 09/28/2005

OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
CHAI, LONGBIT	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 09/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/059,217	HASHIMOTO ET AL.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 August 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1 – 12 have been presented for examination. Claim 7 has been amended in an amendment filed 8/17/2005.

Response to Arguments

1. Applicant's arguments filed on 8/17/2005 with respect to the subject matter of the instant claims have been fully considered but are not persuasive.

2. As per claim 10, Applicant remarks Hartman does not disclose the claimed meta-level information. Examiner disagrees because Hartman teaches memory segment registers includes an indication flag of whether the code / data /stack segment is encrypted or not as well as the storage for corresponding encryption / decryption key (Hartman: Column 6 Line 1 – 8). Therefore, the indication flag and the key storage information as a whole are considered as the meta-level information.

3. As per claim 1, Applicant asserts Hartman in view of Alexander fails to teach the asynchronous interruption used to notify a completion of a key registration to the processor core when the key registration is completed (Page 7, 5th Para). Examiner notes Applicant's arguments have been fully considered but are not persuasive because (a) the Hartman reference is relied upon providing a mechanism that upon a completion of a key registration to the processor core when the key registration is completed, a clear copy of the media master key is then stored into a secure physical memory region (Hartman: Column 4 Line 50 – 57: the master key (i.e. instruction key) is saved into a

secure physical region after being decrypted by the private key – this is considered as equivalent to a registration process), and (b) Alexander is relied upon providing a SMI interrupt (System Management Interrupt) to unlock the flash memory to update (or rewrite) protected information in flash memory (Alexander: Column 5 Line 58 – Column 6 Line 2). Therefore Hartman in view of Alexander does teach the asynchronous interruption used to notify a completion of a key registration to the processor core when the key registration is completed.

4. As per claim 2 and 3, Applicant asserts Hartman fails to teach an instruction cache memory configured to store a cache line containing a part of the instructions of the program in correspondence to the specific program identifier. Examiner notes Hartman teaches the non-encrypted instructions (after decryption) are directly stored in the internal memory cache (Hartman: Column 3 Line 56 – 58) and each of the desired media has the media identifier (Hartman: Column 4 Line 39 – 40: a media identifier is considered as a program ID). Therefore, Hartman in view of Alexander does teach an instruction cache memory configured to store a cache line containing a part of the instructions of the program in correspondence to the specific program identifier.

5. As per claim 4, Applicant asserts Hartman fails to teach chain information indicating chain relationships among encryption blocks. Examiner notes Hartman teaches a variety of program segments classified as code segments, data segments and stack segments contain the media master key that is to be used in decryption or encryption of information in the corresponding memory segments (Hartman: Column 5 Line 51 – 55 and Column 6 Line 9 – 15: each one of encrypted multiple segments can

be considered as a encryption block , where the relationships among the code segment, data segment and stack segment must be closely-tied to assure the proper operation of the system with respect to normal operations and context saving operations).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraph of 35 U.S.C. 102 that forms the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 10 – 12 are rejected under 35 U.S.C. 102(b) as being anticipated by Hartman (Patent Number: 5224166).

As per claim 10, Hartman teaches a microprocessor internally having a secret key specific to the microprocessor that cannot be read out to an external, the microprocessor comprising:

a processor core configured to execute instructions of a program including plaintext instructions and encrypted instructions, the encrypted instructions being encrypted by using an instruction key specific to the program (Hartman, Column 3 Line 18 – 20 and Column 4 Line 20 – 22: MMK key is equivalent to the instruction key); and

a key management unit configured to carry out a key registration for reading out from an external memory a distribution key that is obtained in advance by encrypting the instruction key and a meta-level information integrally by using a public key

corresponding to the secret key, decrypting the distribution key by using the secret key to obtain the instruction key and the meta-level information (Hartman, Column 3 Line 35 – 57 and Column 6 Line 1 – 8: Examiner disagrees because Hartman teaches memory segment registers includes an indication flag of whether the code / data /stack segment is encrypted or not and the storage for corresponding encryption / decryption key (Hartman: Column 6 Line 1 – 8). Therefore, the indication flag and the key storage information as a whole are considered as the meta-level information), and registering the instruction key and the meta-level information in correspondence to a specific program identifier for identifying the program into a key table (Hartman, Column 4 Line 53 – 57 and Column 5 Line 59 – 64: the master key (i.e. instruction key) is saved into a secure physical region after being decrypted by the private key – this is considered as equivalent to a registration process).

As per claim 11, Hartman further teaches the key management unit registers the meta-level information which is a feedback key to be used in obtaining a feedback information by encrypting the instruction key when the feedback information is to be written into the external memory at a time of a context saving (Hartman, Column 5 Line 59 – 64, Column 6 Line 5 Line 8 and Column 6 Line 9 – 15: stack segment is used during the context switching of the CPU operation due to a context saving).

As per claim 12, Hartman further teaches the key management unit registers the meta-level information which is a perpetuation flag indicating whether or not to permit a

context saving in which the instruction key is encrypted by using a prescribed secret key of the microprocessor and written into the external memory (Hartman, Column 7 Line 38 – 40 and Column 5 Line 54: a set flag associated with the stack segment which is related to context saving).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1 – 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hartman (Patent Number: 5224166), in view of Alexander (Patent Number: 6188602).

As per claim 1, Hartman teaches a microprocessor internally having a secret key specific to the microprocessor that cannot be read out to an external, the microprocessor comprising:

a processor core configured to execute instructions of a program including plaintext instructions and encrypted instructions, the encrypted instructions being encrypted by using an instruction key specific to the program (Hartman, Column 3 Line 18 – 20 and Column 4 Line 20 – 22: MMK key is equivalent to the instruction key; and

a key management unit configured to carry out a key registration for reading out from an external memory a distribution key that is obtained in advance by encrypting the instruction key by using a public key corresponding to the secret key, decrypting the distribution key by using the secret key to obtain the instruction key, and registering the instruction key in correspondence to a specific program identifier for identifying the program into a key table (Hartman, Column 4 Line 53 – 57 and Column 5 Line 59 – 64: the master key (i.e. instruction key) is saved into a secure physical region after being decrypted by the private key – this is considered as equivalent to a registration process).

Hartman does not teach using an interrupt to notify asynchronously the completion of the key registration.

Alexander teaches a mechanism to notify a completion of the key registration to the processor core asynchronously by interruption when the key registration is completed, such that the key management unit carries out the key registration during execution of the program by the processor core in which execution of the encrypted instructions starts after the completion of the key registration is notified (Hartman, Column 4 Line 50 – 57, Alexander, Column 1 Line 60 – 65, Column 2 Line 22 – 32 and Column 5 Line 57 – 62: SMI (Interrupt) is used to update the protected information (i.e. medium master key) residing in flash memory via locking / unlocking mode during the system normal computer system operation. Examiner notes (a) the Hartman reference is relied upon providing a mechanism that upon a completion of a key registration to the processor core when the key registration is completed, a clear copy of the media master

key is then stored into a secure physical memory region (Hartman: Column 4 Line 50 – 57), and (b) Alexander is relied upon providing a SMI interrupt (System Management Interrupt) to unlock the flash memory to update or change protected information in flash memory (Alexander: Column 5 Line 58 – Column 6 Line 2)).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Alexander's SMI (System Management Interrupt) within the system of Hartman's instruction key registration process because it offers the advantages of allowing the system to update the protected critical information in parallel to the system normal operation and thereby considerably reducing the platform complexity and improving system reliability (Alexander, Column 2 Line 22 – 32 and Column 1 Line 35 – 36).

As per claim 2, Hartman further teaches an instruction cache memory configured to store a cache line containing a part of the instructions of the program in correspondence to the specific program identifier (Hartman: Column 3 Line 56 – 58 and Column 4 Line 39 – 40: Examiner notes Hartman teaches the non-encrypted instructions (after decryption) are directly stored in the internal memory cache (Hartman: Column 3 Line 56 – 58) and each of the desired media has the media identifier (Hartman: Column 4 Line 39 – 40: a media identifier is considered as a program ID)), and permit reading of the cache line only when the specific program identifier stored in correspondence to the cache line coincides with a program identifier received along with a program reading request from the processor core; wherein the key management unit

is also configured to carry out a flashing of the cache line stored in correspondence to the specific program identifier on the cache memory when the key management unit rewrites the instruction key corresponding to the specific program identifier in the key table (Hartman, Column 3 Line 56 – 58 and Column 7 Line 32 – 35).

As per claim 3, Hartman further teaches the key management unit carries out the flashing in parallel to the key registration, and notifies the completion of the key registration to the processor core when the key registration and the flashing are both completed (Hartman, Column 4 Line 50 – 57, Alexander, Column 1 Line 60 – 65, Column 2 Line 22 – 32 and Column 5 Line 57 – 62: SMI (Interrupt) is used to update the protected information residing in flash memory via locking / unlocking mode during the system normal computer system operation).

As per claim 4, Hartman further teaches an instruction decryption processing unit configured to decrypt the encrypted instructions of the program read out from the external memory, by using the instruction key registered in correspondence to the specific program identifier by the key management unit, according to a chain information indicating chain relationships among encryption blocks in units of which the encrypted instructions are encrypted (Hartman, Figure 2 Element 56, Column 4 Line 20 – 22 , Column 5 Line 51 – 55 and Column 6 Line 9 – 15: each one of encrypted multiple code segments can be considered as a encryption block in units of which the encrypted instructions are encrypted. Examiner notes Hartman teaches a variety of program

segments classified as code segments, data segments and stack segments contain the media master key that is to be used in decryption or encryption of information in the corresponding memory segments and the relationships among the code segment, data segment and stack segment must be closely-tied to assure the proper operation of the system with respect to normal operations and context saving operations).

As per claim 5, Hartman further teaches the key management unit is also configured to register a data key to be used in encrypting/decrypting data for the program in correspondence to the specific program identifier into the key table (Hartman, Column 4 Line 20 – 22, Column 5 Line 54 and Column 6 Line 5 – 8: the master key associated with data segment can be considered as the data key).

As per claim 6, Hartman further teaches a key index conversion unit configured to convert a set of a program identifier and a key type identifier received from the processor core into a corresponding key value index; and a decryption processing unit configured to decrypt encrypted instructions or data of a program specified by the program identifier received from the processor core and read out from the external memory, by using an instruction key or a data key indexed by the corresponding key value index obtained by the key index conversion unit (Hartman, Column 4 Line 20 – 22, Column 5 Line 51 – 55 and Column 6 Line 5 – 15: the key type can be either instruction key, data key or stack (context-switch) key which is associated with code segment, data segment or stack segment as taught by Hartman).

As per claim 7, Hartman further teaches the key index conversion unit converts more than one sets of a program identifier and a key type identifier into an identical key value index (Hartman, Column 4 Line 20 – 22 & Column 4 Line 33 – 34 and Column 5 Line 51 – 55, Column 6 Line 5 – 15).

As per claim 8, Hartman further teaches a cache memory configured to store a part of instructions or data of programs by using key value indexes obtained by the key index conversion unit as cache tags (Hartman, Column 7 Line 32 – 40, Column 4 Line 20 – 22 & Column 4 Line 33 – 34 and Column 5 Line 51 – 55, Column 6 Line 5 – 15: a data cache associated with an encrypted data segment using a flag to associated with the situation whether the corresponding code segment is encrypted or not).

As per claim 9, Hartman further teaches the key management unit is also configured to register a data key to be used in encrypting/decrypting data for the program in correspondence to the specific program identifier into the key table (Hartman, Column 4 Line 20 – 22, Column 5 Line 54 and Column 6 Line 5 – 8: the master key associated with stack segment can be considered as the context-switch key where stack segment is used during the context switching of the CPU operation due to a context saving).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LBC

LBC

Longbit Chai
Examiner
Art Unit 2131

Primary Examiner
AU 2131
9/23/05